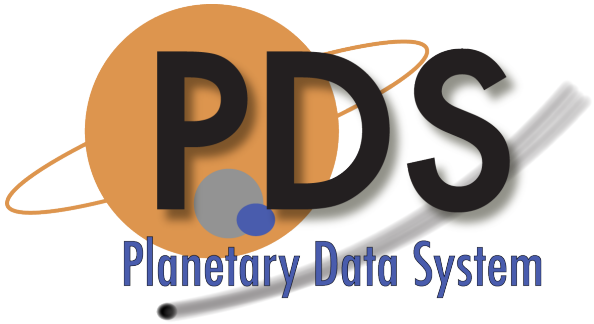

IT Security

MC F2F

April 2014

Dan Crichton, Emily Law, Tom Morgan, Pat Michael

Introduction

- IT security is a growing area of concern for NASA data systems

- While PDS is hosted inside and outside NASA centers, it does present itself as a NASA-based system
  - Recent IT security breaches at the nodes have raised concerns regarding an overall PDS IT security plan
  - PDS MC formed a WG in November, but the WG ended up determining this might require a PDS-wide IT security plan

- PDS carries a level 3 requirement for IT Security
  - 2.10.3: PDS will ensure that appropriate mechanisms are in place to prevent unauthorized users from compromising the integrity of systems and data

Action Item

- 2014-01-13/A (Crichton, 2014-04-10): Check with JPL and Goddard people to determine best course of action for improving computer security.

Progress to date

- Began defining an IT security plan for the PDS
  - Recognize that IT security approaches differ across the nodes
  - Focus on deriving a minimal set of requirements
  - Recognize that many may already be following the practices
  - Recognize that PDS needs to have a more formalized approach to IT security
- Defined a template for capturing IT security plans across the nodes
- Reviewed by GSFC and JPL

Approach

- Worked with the JPL System Administration and IT Security teams to develop a general template based on existing mission IT security plans
  - Generalized for PDS
- NASA centers already have required plans in the system
  - For example, JPL requires Engineering, NAIF and Imaging-JPL to update its plan annually and ensure that all systems are routinely scanned
  - Issue must be resolved to maintain a presence on the network
- Comment: Within the IT security plan, “users” of computing services, infrastructures, etc are node staff not the “PDS users”

Elements of the plan (1)

- *System identification* – purpose
- *Data/Information identification* – type of data
- *Information sharing* – how data is shared with users of the data
- *Risk assessment and analysis* – a description of what is being done, documented vulnerabilities, and the overall threat assessment

Elements of the plan (2)

- *Technical controls* - the technical controls that are being applied to enforce the rules or policies of the system
- *Public access controls* - Describe how the system is protected from public access (e.g, via firewalls, etc)
- *Rules of the system* – how users obtain accounts, remote access rules, privileges, termination, etc
- *Personnel screening* – who is given access and to what
- *Training* – how are users trained about the rules

Elements of the plan (3)

- *Contingency Planning* – Plans and procedures for continuing PDS operations after an incident
- *Incident Response* – procedures on how an incident is handled (e.g., how is notified).
- *System interconnection* – what interactions exist to other systems (e.g., to EN and other node services)
- *Review of security controls* – how is the system audited? (e.g., quarterly network scans for vulnerabilities)
  - Automated checks against an ever increasing set of vulnerabilities in software is critical

Example technical controls

- If there has been no keyboard activity for a fixed period of time, not to exceed 15 minutes, computer systems shall automatically suspend console access, when this capability is provided by the operating system.
- Directories accessed through anonymous FTP shall be configured such that those permitting write access do not allow read or list access.
- Remote access shall be restricted to authorized users.
- Users (or processes acting on behalf of users) shall be assigned the fewest privileges consistent with their assigned duties and functions.
- System log files shall be retained for at least 90 days.
- Successful and failed logins/logoffs shall be recorded in the system log files.
- etc

Recommendations

- Finalize and distribute template.
- Each node file an IT security plan with GSFC as part of their annual report following the template.
- Engineering will write an overall document that describes the minimal capabilities that will reference the node security plans.
- Nodes are encouraged to begin reviewing their IT security practices.